State of Vermont
Incident Handling Procedure

TABLE OF CONTENTS

State of Vermont
Incident Handling Procedure

Introduction

We understand that this document is to be used as a guideline until the CSIRT team can enhance and update this procedure on a regular basis to minimize risk to our environment. All changes to this procedure must me approved by IRMAC before distribution to agencies or departments.

Scope

This document provides general guidelines and procedures for dealing with computer security incidents. The document is meant to provide the State of Vermont computer support personnel with some guidelines on what to do if a security incident is discovered. **The term incident in this document is defined as any irregular or adverse event, which can be electronic, physical, or social that occurs on any part of the State's infrastructure**. Some examples of possible incident categories include: compromise of system integrity; false identity to gain information or passwords, denial of system resources; illegal access to a system or site (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are: One detects:

A strange process running and accumulating a lot of CPU time.

An intruder logged into your system.

A virus has infected your system.

That someone from a remote site is trying to penetrate the system.

The steps involved in handling a security incident are categorized into five stages:

protection of the system;

identification of the problem;

containment of the problem;

eradication of the problem;

recovering from the incident and

follow-up analysis.

The actions taken in some of these stages are common to all types of security incidents and are discussed under *General Procedures*. Computer Crimes as defined in Section 1.13 V.S.A. chapter 87 of Vermont Statutes may or may not qualify when an incident occurs. Inappropriate use of electronic communications by state staff is defined in the Personnel Policies and Procedures manual any violation of this policy should involve the commissioner or department head and your personnel officer.

AREAS OF RESPONSIBILITY

In many cases, the actions outlined in this guideline will not be performed by a single person on a single system. Many people may be involved during the course of an active security incident which affects several of the state systems at one time (i.e., a worm attack). The Office of the CIO should always be involved in the investigation of any security incident and will be contacted by CSIRT.

Each Agency or Department will designate a security contact that will contact the Vermont Computer Security Incident Response Team (CSIRT). CSIRT can be contacted by sending Email to: CSIRT@.state.vt.us or calling

802-828-3544. CSIRT will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and clean-up are responsible for providing any needed information to members of the incident coordination team. Any directives given by a member of the CSIRT will supersede this document.

IMPORTANT CONSIDERATIONS

A computer security incident can occur at anytime of the day or night, although most hacker incidents occur during the off hours when hackers do not expect system managers to be watching their operation. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident. Providing information to the wrong people could have undesirable side effects. The *General Procedures* section discusses the policy on release of information.

GENERAL PROCEDURES

This section discusses procedures that are common for all types of security incidents. The potential exists that the information you capture or record may be essential to a criminal investigation or prosecution. Always maintain the integrity of the data and follow evidentiary rules.

KEEP A LOG BOOK

Logging of information is critical in situations that may eventually involve local and state, as well as federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

* Dates and times of incident-related phone calls.

* Dates and times when incident-related events were discovered or occurred.

* Amount of time spent working on incident-related tasks.

* People you have contacted or have contacted you.

* Names of systems, programs or networks that have been affected.

INFORM THE APPROPRIATE PEOPLE

Informing the appropriate people is of extreme importance. There are some actions that can only be authorized by the department IT manager. The CSIRT also has the responsibility to inform other sites about an incident that may effect them.

LIST OF CONTACTS

CSIRT ? CSIRT@.state.vt.us **or 802-828-3544**

Department/Agency IT Manager or lead security designee

RELEASE OF INFORMATION

Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. The Office of the CIO working with CSIRT, the specific department commissioner, and agency secretary or office director must authorize all release of information. All requests for press releases must be forwarded to the commissioner level. Keep in mind, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be involved with security at another site. All suspicious requests for information should be forwarded to the commissioner level. If there is any doubt about whether you can release a specific piece of information contact the commissioner's office, a member of CSIRT or the Office of the CIO

FOLLOW-UP ANALYSIS

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). A set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by CSIRT and distributed to all appropriate personnel.

REPORTING

The CSIRT is responsible for updating the state technical community through IRMAC and other direct methods.

INCIDENT SPECIFIC PROCEDURES

This section discusses the procedure for handling virus, worm and hacker incidents.

VIRUS AND WORM INCIDENTS

Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes, thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, then proceed as if the attack was worm related.

Step 1: Isolate the System

Isolate infected system(s) from GOVnet as soon as possible. If a worm is suspected, then a decision must be made to disconnect the server(s) from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since some or all of GOVnet will be disconnected from sites which may have patches. The Office of the CIO must authorize the isolation of the entire wide area network from the outside world. **Log all actions.**

Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.

Step 2: Notify Appropriate People

Notify CSIRT as soon as possible. Notify your departmental designated authority (IT Manager or other designee. If unable to reach him/her within one hour, contact the backup person. The CSIRT and IT

Manager will then be responsible for notifying other appropriate personnel.

Step 3: Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Each server/operating system configuration should have a defined series of steps to follow that includes saving log files, history and/or active processes. Also, get a listing of all active network connections.

If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files.

Run the CSIRT recommended security software on the infected system(s) to identify other possible problems such as altered system files, new programs or hidden special files.

If other sites have been involved at this point, they may have helpful information on the problem and possible short-term solutions. Also, any helpful information gained about the virus or worm will be passed along to Internet Computer Emergency Response Team (CERT) sites by the CSIRT. Log all actions.

Step 4: Contain the virus or worm

All suspicious processes should now be halted and removed from the system. Make a full dump of the system and store in a safe place. The tapes should be carefully labeled so unsuspecting people will not use them in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all state systems have been inoculated and/or the other internet sites have been cleaned up and inoculated. **Log all actions.**

Step 5: Inoculate the System(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the tasks of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. **Log all actions.**

Step 6: Return to a Normal Operating Mode

Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

Step 7: Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). A set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the CSIRT and distributed to all appropriate personnel.

HACKER INCIDENTS

Responding to hacker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker incident needs to be addressed as a real threat to the state's computing and communication infrastructure.

Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker session is the most severe and must be dealt with as soon as possible.

There are two methods for dealing with an active hacker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the hacker to continue his probe/attack and attempt to gather information that will lead to an identification and possible criminal conviction. The method used to handle a hacker incident will be determined by the level of understanding of the risks involved.

(A) Attempted Probes into a State of Vermont System

Incidents of this type would include: repeated login attempts, repeated ftp, or telnet commands, and repeated dial-back attempts.

Step 1: Identify Problem

Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files and store them in a safe place. Capture process status information in a file and then store the file in a safe place. **Log all actions.**

Step 2: Notify appropriate people

Notify the CSIRT and your IT Manager within 30 minutes. After consultation with CSIRT you may need to notify the police authority with jurisdiction at the location of the attack. If one of the CSIRT members cannot be reached then your IT Manager will have alternate procedures for notifying other levels of management.

Step 3: Identify Hacker

If the source of the attacks or if the hacker can be identified, then CSIRT (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identify of the hacker. **Log all actions.**

Step 4: Notify CERT

If the source of the attacks can not be identified, then the CSIRT will contact the Internet CERT and provide them with information concerning the attack. ***NOTE **-** Release of information must be approved by the Office of the CIO in conjunction with the commissioner of the department(s) involved. **Log all actions.**

Step 5: Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). A set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the incident coordination team and distributed to all appropriate personnel.

(B) Active Hacker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by CSIRT and the departmental I.T. Manager or designee. The decision will be based on the availability of qualified personnel to monitor and observe the hacker and the level of risk involved.

Step 1: Notify Appropriate People

Notify a member of the CSIRT as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The CSIRT will then be responsible for notifying other appropriate personnel. The team, with help from the involved departmental technical staff, will be responsible for trying to assess what the hacker is after and the risks involved in letting the hacker continue his/her activity. Other state personnel may be contacted depending on the location and activity of the hacker and the risks involved. Based on the decision, follow the procedures in Options 1 and 2 below.

Option 1: Removal of Hacker From the System

Step 2: Snap-shot the System

Make copies of all audit trail information such as system logs files and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. **Log all actions.**

Step 3: Lock Out the Hacker

Kill all active processes for the hacker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker. At this stage, the hacker should be locked out of the system. **Log all actions.**

Step 4: Restore the System

Restore the system to a normal state. Restore any data or files that the hacker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the logbook for this incident. **Log all actions.**

Step 5: Notify Other Agencies

CSIRT will report the incident to CERT. ***NOTE- Release of information must be approved by the Office of the CIO working with the department commissioner(s). **Log all actions**.

Step 6: Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). A set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the incident coordination team and distributed to all appropriate personnel.

Option 2: Monitoring of Hacker Activity

There are no set procedures for monitoring the activity of a hacker. Each incident will be dealt with on a case by case basis. The CSIRT or the person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker?s activities and have him removed from the system(s), the steps outlined in Option 1above should be followed.

(C) Evidence of Past Incidents

In the case of where an incident is discovered after the fact, there is not always a lot of evidence available to identify who the person was or how they gained access to the system. If you should discover that someone had successfully broke into a state system, notify the CSIRT, your IT Manager or designee and after consulting with CSIRT you may need to contact your local police authority within one working day. The CSIRT will be responsible for notifying the appropriate people and investigating the incident.

SOCIAL INCIDENTS

Responding to social incidents is somewhat different than responding to a worm or virus incident. Some hackers will use techniques to trick people into revealing passwords or other information that compromises a target systems security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem. This type of hacking is generally referred to as social engineering and needs to be addressed as a real threat to the computing and communication infrastructure. Once a hacker obtains an employee?s password they will go unnoticed which could cause severe damage and disruption. If you receive a suspicious call or request (through other means) to gain access to a state system or network you should:

Step 1: Notify Appropriate People

Notify a member of the CSIRT and your departmental security designee as soon as possible. The CSIRT will then be responsible for notifying other appropriate personnel. The team, with help from the involved departmental technical staff, will be responsible for trying to assess what the hacker is after and the risks involved in letting the hacker continue his/her activity. Other state personnel may be contacted depending on the location and activity of the hacker and the risks involved. **Log all actions.**

PHYSICAL INCIDENTS

Responding to physical incidents is something we all need to be aware of on a daily basis. Any suspicious activity such as unattended people wandering around or unlocked doors that are normally locked could be a potential security risk. This type of incident needs to be addressed as a real threat to the state?s computing and communication infrastructure.

Step 1: Identify Potential Risk

Confront individuals and ask for identification and the purpose for the visit. Do not attempt any contact if you feel you are in personal danger. When forceful entry of a site has occurred, contact local police authority with jurisdiction at the location of the incident. **Log all actions.**

Step 2: Notify Appropriate People

If the incident is a physical intrusion notify a member of the CSIRT and your departmental security designee as soon as possible. The CSIRT will then be responsible for notifying other appropriate personnel. Other state personnel may be contacted depending on the location, suspicious activity, security breach and the risks involved. **Log all actions.**

Incident Response Checklist

✍✍ Potential Incident Verified

✍✍ Contact department/agency security staff
- ✍✍ I.T. Manager -
- ✍✍ [designee/others by department procedure] -

✍✍Security designee will contact CSIRT member
- ✍✍CSIRT - Email to: CSIRT@.state.vt.us or call 802-828-3544

✍✍Isolate system(s) from GOVnet [unless CSIRT decision is to leave the system connected to monitor active hacker]

✍✍Begin a log book - who/ what / when / where

✍✍Identify type of Incident - Virus, worm, hacker

✍✍Preliminary estimate of extent of problem, number of systems

✍✍In the event of a crime, as defined by 1.13 VSA Chapter 87, notify local authorities.

✍✍Follow server/operating system specific procedures to snapshot the system

✍✍Inoculate/restore the system

✍✍Close the vulnerability and assure all patches have been installed

✍✍Return to normal operations

✍✍Prepare report and conduct follow-up analysis, deliver a copy to CSIRT

✍✍Revise prevention and screening procedures

Remember to log all actions.